

# STABILITY RESULT FOR SETS WITH $3A \neq \mathbb{Z}_5^n$

VSEVOLOD F. LEV

**ABSTRACT.** As an easy corollary of Kneser's Theorem, if  $A$  is a subset of the elementary abelian group  $\mathbb{Z}_5^n$  of density  $5^{-n}|A| > 0.4$ , then  $3A = \mathbb{Z}_5^n$ . We establish the complementary stability result: if  $5^{-n}|A| > 0.3$  and  $3A \neq \mathbb{Z}_5^n$ , then  $A$  is contained in a union of two cosets of an index-5 subgroup of  $\mathbb{Z}_5^n$ . Here the density bound 0.3 is sharp.

Our argument combines combinatorial reasoning with a somewhat non-standard application of the character sum technique.

## 1. INTRODUCTION

For a subset  $A$  of an (additively written) abelian group  $G$ , and a positive integer  $k$ , denote by  $kA$  the  $k$ -fold sumset of  $A$ :

$$kA := \{a_1 + \cdots + a_k : a_1, \dots, a_k \in A\}.$$

How large can  $A$  be given that  $kA \neq G$ ? Assuming that  $G$  is finite, let

$$M_k(G) := \max\{|A| : A \subseteq G, kA \neq G\}.$$

This quantity was introduced and completely determined by Bajnok in [B15]. The corresponding result, expressed in [B15] in a somewhat different notation, can be easily restated in our present language.

**Theorem 1** (Bajnok [B15, Theorem 6]). *For any finite abelian group  $G$  and integer  $k \geq 1$ , writing  $m := |G|$ , we have*

$$M_k(G) = \max \left\{ \left( \left\lfloor \frac{d-2}{k} \right\rfloor + 1 \right) \frac{m}{d} : d \mid m \right\}$$

(where  $\lfloor \cdot \rfloor$  is the floor function, and the maximum extends over all divisors  $d$  of  $m$ ).

Once  $M_k(G)$  is known, it is natural to investigate the associated stability problem: what is the structure of those  $A \subseteq G$  with  $kA \neq G$  and  $|A|$  close to  $M_k(G)$ ?

---

2010 *Mathematics Subject Classification.* Primary: 11P70; secondary: 20K01, 05D99, 11B75.

*Key words and phrases.* Sumsets, stability, finite abelian groups, Kneser's theorem.

There are two “trivial” ways to construct large subsets  $A \subseteq G$  satisfying  $kA \neq G$ . One is to simply remove elements from a yet larger subset with this property; another is to fix a subgroup  $H < G$  and a set  $\overline{A} \subseteq G/H$  with  $k\overline{A} \neq G/H$ , and define  $A \subseteq G$  to be the full inverse image of  $\overline{A}$  under the canonical homomorphism  $G \rightarrow G/H$ . It is thus natural to consider as “primitive” those subsets  $A \subseteq G$  with  $kA \neq G$  which are maximal subject to this property and, in addition, cannot be obtained by the lifting procedure just described.

To proceed, we recall that the *period* of a subset  $A \subseteq G$ , denoted  $\pi(A)$  below, is the subgroup consisting of all elements  $g \in G$  such that  $A + g = A$ :

$$\pi(A) := \{g \in G : A + g = A\}.$$

Alternatively,  $\pi(A)$  can be defined as the (unique) maximal subgroup such that  $A$  is a union of its cosets. The set  $A$  is called aperiodic if  $\pi(A) = \{0\}$ , and periodic otherwise.

It is readily seen that a set  $A \subseteq G$  with  $kA \neq G$  can be obtained by lifting if and only if it is periodic. Accordingly, motivated by the discussion above, for a finite abelian group  $G$  and integer  $k \geq 1$ , we define  $\mathbf{N}_k(G)$  to be the largest size of an aperiodic subset  $A \subseteq G$  satisfying  $kA \neq G$  and maximal under this condition:

$$\begin{aligned} \mathbf{N}_k(G) := \max\{|A| : A \subseteq G, \pi(A) = \{0\}, \\ kA \neq G \text{ and } k(A \cup \{g\}) = G \text{ for each } g \in G \setminus A\} \end{aligned}$$

(subject to the agreement that  $\max \emptyset = 0$ ). Clearly, we have  $\mathbf{N}_k(A) \leq \mathbf{M}_k(A)$ , and if the inequality is strict (which is often the case), then determining  $\mathbf{N}_k(G)$  is, in fact, a stability problem; for if  $kA \neq G$  and  $|A| > \mathbf{N}_k(G)$ , then  $A$  is contained in the set obtained by lifting a subset  $\overline{A} \subseteq G/H$  with  $k\overline{A} \neq G/H$ , for a proper subgroup  $H < G$ .

The quantity  $\mathbf{N}_k(G)$  is quite a bit subtler than  $\mathbf{M}_k(G)$  and indeed, the latter can be easily read off from the former; specifically, it is not difficult to show that

$$\mathbf{M}_k(G) = \max\{|H| \cdot \mathbf{N}_k(G/H) : H \leq G\}.$$

An invariant tightly related to  $\mathbf{N}_k(G)$  was studied in [KL09]. To state (the relevant part of) the results obtained there, following [KL09], we denote by  $\text{diam}^+(G)$  the smallest non-negative integer  $k$  such that every generating subset  $A \subseteq G$  satisfies  $\{0\} \cup A \cup \dots \cup kA = G$ ; that is,  $k(A \cup \{0\}) = G$ . As shown in [KL09, Theorem 2.1],

if  $G$  is of type  $(m_1, \dots, m_r)$  with positive integers  $m_1 \mid \dots \mid m_r$ , then

$$\text{diam}^+(G) = \sum_{i=1}^r (m_i - 1). \quad (1)$$

**Theorem 2** ([KL09, Theorem 2.5 and Proposition 2.8]). *For any finite abelian group  $G$  and integer  $k \geq 1$ , we have*

$$\mathbf{N}_k(G) \leq \left\lfloor \frac{|G| - 2}{k} \right\rfloor + 1.$$

*If  $G$  is cyclic of order  $|G| \geq k + 2$  then, indeed, equality holds.*

**Theorem 3** ([KL09, Theorem 2.4]). *For any finite abelian group  $G$  and integer  $k \geq 1$ , denoting by  $\text{rk}(G)$  the smallest number of generators of  $G$ , we have*

$$\mathbf{N}_k(G) = \begin{cases} |G| - 1 & \text{if } k = 1, \\ \lfloor \frac{1}{2} |G| \rfloor & \text{if } k = 2 < \text{diam}^+(G), \\ \text{rk}(G) + 1 & \text{if } k = \text{diam}^+(G) - 1, \\ 1 & \text{if } k \geq \text{diam}^+(G) \text{ and } |G| \text{ is prime,} \\ 0 & \text{if } k \geq \text{diam}^+(G) \text{ and } |G| \text{ is composite.} \end{cases}$$

**Theorem 4** ([KL09, Theorem 2.7]). *For any finite abelian group  $G$  with  $\text{diam}^+(G) \geq 4$ , we have*

$$\mathbf{N}_3(G) = \begin{cases} \frac{1}{3} |G| & \text{if 3 divides } |G|, \\ \frac{1}{3} (|G| - 1) & \text{if every divisor of } |G| \text{ is congruent to 1 modulo 3.} \end{cases}$$

In Section 4, we explain exactly how Theorems 2–4 follow from the results of [KL09].

Theorem 4 is easy to extend to show that, in fact, the equality

$$\mathbf{N}_3(G) = \frac{1}{3} (|G| - 1)$$

holds true for any finite abelian group  $G$  decomposable into a direct sum of its cyclic subgroups of orders congruent to 1 modulo 3. Here the upper bound is an immediate consequence of Theorem 2, while a construction matching this bound is as follows.

*Example 1.* Suppose that  $G = G_1 \oplus \dots \oplus G_n$ , where  $G_1, \dots, G_n \leq G$  are cyclic with  $|G_i| \equiv 1 \pmod{3}$ , for each  $i \in [1, n]$ . Write  $|G_1| = 3m + 1$  and let  $H := G_2 \oplus \dots \oplus G_n$  so that  $G = G_1 \oplus H$ . Assuming that  $\mathbf{N}_3(H) = \frac{1}{3}(|H| - 1)$ , find an aperiodic subset  $S \subseteq H$  with  $|S| = \frac{1}{3}(|H| - 1)$ , such that  $3S \neq H$  and  $S$  is maximal subject to this last condition. (If  $n = 1$  and  $H$  is the trivial group, then take  $S = \emptyset$ .) Fix a generator  $e \in G_1$ , and consider the set

$$A := H \cup (e + H) \cup \dots \cup ((m - 1)e + H) \cup (me + S) \subseteq G.$$

It is readily seen that  $3A \neq G$  and  $A$  is maximal with this property. Furthermore,

$$|A| = m|H| + |S| = \frac{1}{3}(|G| - 1)$$

implying  $\gcd(|A|, |G|) = 1$ , whence  $A$  is aperiodic. As a result,  $N_3(G) \geq |A| = \frac{1}{3}(|G| - 1)$ .

Applying this construction recursively, we conclude that  $N_3(G) \geq \frac{1}{3}(|G| - 1)$  whenever  $G$  is a direct sum of its cyclic subgroups of orders congruent to 1 modulo 3.

In contrast with Theorem 3 establishing the values of  $N_1(G)$  and  $N_2(G)$  for all finite abelian groups  $G$ , Theorem 4 and the remark following it address certain particular groups only, and it is by far not obvious whether  $N_3(G)$  can be found explicitly in the general case. In this situation it is interesting to investigate at least the most “common” families of groups not covered by Theorem 4 and Example 1, such as the homocyclic groups  $\mathbb{Z}_m^n$  with  $m \equiv 2 \pmod{3}$ .

An important result of Davydov and Tombak [DT89], well known for its applications in coding theory and finite geometries, settles the problem for the groups  $\mathbb{Z}_2^n$ ; stated in our terms, it reads as

$$N_3(\mathbb{Z}_2^n) = 2^{n-2} + 1, \quad n \geq 4.$$

The goal of this paper is to resolve the next major open case, determining the value of  $N_3(\mathbb{Z}_5^n)$ . To state our main result, we need two more observations.

*Example 2.* If  $A \subset \mathbb{Z}_5^n$  is a union of two cosets of a subgroup of index 5, then  $3A \neq \mathbb{Z}_5^n$ , and  $A$  is maximal with this property: that is,  $3(A \cup \{g\}) = \mathbb{Z}_5^n$  for every element  $g \in \mathbb{Z}_5^n \setminus A$ .

We omit the (straightforward) verification.

*Example 3.* Let  $n \geq 2$  be an integer. Fix a subgroup  $H < \mathbb{Z}_5^n$  of index 5, an element  $e \in \mathbb{Z}_5^n$  with  $\mathbb{Z}_5^n = H \oplus \langle e \rangle$ , and a set  $S \subseteq H$  such that  $|S| = (|H| - 1)/2$  and  $0 \notin 2S$ . Finally, let

$$A := (H \setminus \{0\}) \cup (e + S) \cup \{2e\}.$$

We have then  $|A| = (3 \cdot 5^{n-1} - 1)/2$ , and hence  $A$  is aperiodic. Also, it is easily verified that  $3A = \mathbb{Z}_5^n \setminus \{4e\}$ , and that  $4e \in 3(A \cup \{g\})$  for any  $g \in \mathbb{Z}_5^n \setminus A$ .

The last example shows that

$$N_3(\mathbb{Z}_5^n) \geq \frac{1}{2}(3 \cdot 5^{n-1} - 1), \quad n \geq 2.$$

With this estimate in view, we can eventually state the main result of our paper.

**Theorem 5.** *Suppose that  $n$  is a positive integer, and  $A \subseteq \mathbb{Z}_5^n$  satisfies  $3A \neq \mathbb{Z}_5^n$ . If  $|A| > 3 \cdot 5^{n-1}/2$ , then  $A$  is contained in a union of two cosets of a subgroup of index 5. Consequently, in view of Theorem 2 and Example 3,*

$$\mathbf{N}_3(\mathbb{Z}_5^n) = \begin{cases} 2 & \text{if } n = 1, \\ \frac{1}{2}(3 \cdot 5^{n-1} - 1) & \text{if } n \geq 2. \end{cases}$$

We collect several basic results used in the proof of Theorem 5 in the next section; the proof itself is presented in Section 3. In Section 4 we explain exactly how Theorems 2–4 follow from the results of [KL09].

In conclusion, we remark that any finite abelian group not addressed in Example 1 has a direct-summand subgroup of order congruent to 2 modulo 3, and Example 3 generalizes onto “most” of such groups, as follows.

*Example 4.* Suppose that the finite abelian group  $G$  has a direct-summand subgroup  $G_1 < G$  of order  $|G_1| = 3m + 2$  with integer  $m \geq 1$ , and find a generator  $e \in G_1$  and a subgroup  $H < G$  such that  $G = G_1 \oplus H$ .

Assuming first that  $|H|$  is odd, fix a subset  $S \subseteq H$  with  $0 \notin 2S$  and  $|S| = \frac{1}{2}(|H| - 1)$ , and let

$$\begin{aligned} A := H \cup (e + H) \cup \cdots \cup ((m-2)e + H) \\ \cup ((m-1)e + (H \setminus \{0\})) \cup (me + S) \cup \{(m+1)e\}. \end{aligned}$$

A simple verification shows that  $(3m+1)e \notin 3A$  and  $A$  is maximal with this property. Furthermore, since there is a unique  $H$ -coset containing exactly  $|H| - 1$  elements of  $A$ , we have  $\pi(A) \leq H$ , and since there is an  $H$ -coset containing exactly one element of  $A$ , we actually have  $\pi(A) = \{0\}$ . Therefore,

$$\mathbf{N}_3(G) \geq |A| = (m|H| - 1) + |S| + 1 = \frac{2m+1}{6m+4}|G| - \frac{1}{2}.$$

Assuming now that  $|H|$  is even, fix arbitrarily an element  $g \in H$  not representable in the form  $g = 2h$  with  $h \in H$ , find a subset  $S \subseteq H$  with  $g \notin 2S$  and  $|S| = \frac{1}{2}|H|$ , and let

$$\begin{aligned} A := H \cup (e + H) \cup \cdots \cup ((m-2)e + H) \\ \cup ((m-1)e + (H \setminus \{g\})) \cup (me + S) \cup \{(m+1)e\}. \end{aligned}$$

We have then  $(3m+1)e + g \notin 3A$ , and  $A$  is maximal with this property. Also, it is not difficult to see that  $\pi(A) = \{0\}$ . Hence,

$$\mathbf{N}_3(G) \geq |A| = (m|H| - 1) + |S| + 1 = \frac{2m+1}{6m+4}|G|.$$

## 2. AUXILIARY RESULTS

For subsets  $A$  and  $B$  of an abelian group, we write  $A + B := \{a + b : a \in A, b \in B\}$ .

The following immediate corollary from the pigeonhole principle will be used repeatedly.

**Lemma 1.** *If  $A$  and  $B$  are subsets of a finite abelian group  $G$  such that  $A + B \neq G$ , then  $|A| + |B| \leq |G|$ .*

An important tool utilized in our argument is the following result that we will refer to below as *Kneser's Theorem*.

**Theorem 6** ([Kn53, Kn55]). *If  $A$  and  $B$  are finite subsets of an abelian group, then*

$$|A + B| \geq |A| + |B| - |\pi(A + B)|.$$

Finally, we need the following lemma used in Kneser's original proof of his theorem.

**Lemma 2** ([Kn53, Kn55]). *If  $A$  and  $B$  are finite subsets of an abelian group, then*

$$|A \cup B| + |\pi(A \cup B)| \geq \min\{|A| + |\pi(A)|, |B| + |\pi(B)|\}.$$

## 3. PROOF OF THEOREM 5

We start with a series of results preparing the ground for the proof. Unless explicitly indicated, at this stage we do not assume that  $A$  satisfies the assumptions of Theorem 5.

For subsets  $A, B \subseteq \mathbb{Z}_5^n$  with  $0 < |B| < \infty$ , by the *density* of  $A$  in  $B$  we mean the quotient  $|A \cap B|/|B|$ . In the case where  $B = \mathbb{Z}_5^n$ , we speak simply about the *density* of  $A$ .

**Proposition 1.** *Let  $n \geq 1$  be an integer, and suppose that  $A \subseteq \mathbb{Z}_5^n$  is a subset of density larger than 0.3. If  $3A \neq \mathbb{Z}_5^n$ , then  $A$  cannot have non-empty intersections with exactly three cosets of an index-5 subgroup of  $\mathbb{Z}_5^n$ .*

*Proof.* Assuming that  $3A \neq \mathbb{Z}_5^n$  and  $F < \mathbb{Z}_5^n$  is an index-5 subgroup such that  $A$  intersects exactly three of its cosets, we obtain a contradiction.

Translating  $A$  appropriately, we assume without loss of generality that  $0 \notin 3A$ . Fix  $e \in \mathbb{Z}_5^n$  such that  $\mathbb{Z}_5^n = F \oplus \langle e \rangle$ , and for  $i \in [0, 4]$  let  $A_i := (A - ie) \cap F$ ; thus,  $A = A_0 \cup (e + A_1) \cup (2e + A_2) \cup (3e + A_3) \cup (4e + A_4)$  with exactly three of the sets  $A_i$  non-empty. Considering the action of the automorphisms of  $\mathbb{Z}_5$  on its two-element subsets (equivalently, passing from  $e$  to  $2e, 3e$ , or  $4e$ , if necessary), we further assume that one of the following holds:

- (i)  $A_2 = A_3 = \emptyset$ ;
- (ii)  $A_3 = A_4 = \emptyset$ ;
- (iii)  $A_0 = A_4 = \emptyset$ .

We consider these three cases separately.

Case (i):  $A_2 = A_3 = \emptyset$ . In this case we have  $A = A_0 \cup (e + A_1) \cup (4e + A_4)$ , and from  $0 \notin 3A$  we obtain  $0 \notin A_0 + A_1 + A_4$ . Consequently,  $|A_0| + |A_1 + A_4| \leq |F|$  by Lemma 1, whence

$$|A_0| + \max\{|A_1|, |A_4|\} \leq |F|$$

and similarly,

$$\begin{aligned} |A_1| + \max\{|A_0|, |A_4|\} &\leq |F|, \\ |A_4| + \max\{|A_0|, |A_1|\} &\leq |F|. \end{aligned}$$

Thus, denoting by  $M$  the largest, and  $m$  the second largest of the numbers  $|A_0|, |A_1|$ , and  $|A_4|$ , we have  $M + m \leq |F|$ . It follows that

$$|A| = |A_0| + |A_1| + |A_4| \leq \frac{3}{2}(M + m) \leq \frac{3}{2}|F|,$$

contradicting the density assumption  $|A| > 0.3 \cdot 5^n$ .

Case (ii):  $A_3 = A_4 = \emptyset$ . In this case from  $0 \notin 3A$  we get  $3A_0 \neq F$  and  $A_1 + 2A_2 \neq F$ , whence also  $2A_0 \neq F$  and  $A_1 + A_2 \neq F$  and therefore  $2|A_0| \leq |F|$  and  $|A_1| + |A_2| \leq |F|$  by Lemma 1. This yields

$$|A| = |A_0| + |A_1| + |A_2| \leq \frac{3}{2}|F|,$$

a contradiction as above.

Case (iii):  $A_0 = A_4 = \emptyset$ . Here we have  $2A_1 + A_3 \neq F$  and  $A_1 + 2A_2 \neq F$  implying  $|A_1| + |A_3| \leq |F|$  and  $2|A_2| \leq |F|$ , respectively. This leads to a contradiction as in Case (ii).  $\square$

**Lemma 3.** *Let  $n \geq 1$  be an integer, and suppose that  $A \subseteq \mathbb{Z}_5^n$ . If  $2A$  has density smaller than 0.5, then  $A$  has density smaller than 0.25.*

*Proof.* Write  $H := \pi(2A)$  and let  $\varphi_H: \mathbb{Z}_5^n \rightarrow \mathbb{Z}_5^n/H$  be the canonical homomorphism. Applying Kneser's theorem to the set  $A+H$  and observing that  $2(A+H) = 2A+H = 2A$ , we get  $|2A| \geq 2|A+H| - |H|$ , whence  $|\varphi_H(2A)| \geq 2|\varphi_H(A)| - 1$ . If the density of  $2A$  in  $\mathbb{Z}_5^n$  is smaller than 0.5, then so is the density of  $\varphi_H(2A)$  in  $\mathbb{Z}_5^n/H$  (in fact, the two densities are equal); hence, in this case

$$\frac{1}{2}|\mathbb{Z}_5^n/H| > |\varphi_H(2A)| \geq 2|\varphi_H(A)| - 1.$$

This yields  $|\varphi_H(A)| < \frac{1}{4}(|\mathbb{Z}_5^n/H| + 2)$  and thus, indeed,  $|\varphi_H(A)| < \frac{1}{4}|\mathbb{Z}_5^n/H|$  as  $|\mathbb{Z}_5^n/H| \equiv 1 \pmod{4}$ . It remains to notice that the density of  $A$  in  $\mathbb{Z}_5^n$  does not exceed the density of  $\varphi_H(A)$  in  $\mathbb{Z}_5^n/H$ .  $\square$

**Proposition 2.** *Let  $n \geq 1$  be an integer, and suppose that  $A \subseteq \mathbb{Z}_5^n$  is a subset of density larger than 0.3, such that  $3A \neq \mathbb{Z}_5^n$ . If  $A$  has density larger than 0.5 in a coset of an index-5 subgroup  $F < \mathbb{Z}_5^n$ , then  $A$  has non-empty intersections with at most three cosets of  $F$ .*

*Proof.* Fix  $e \in \mathbb{Z}_5^n$  with  $\mathbb{Z}_5^n = F \oplus \langle e \rangle$ , and for  $i \in [0, 4]$  set  $A_i := (A - ie) \cap F$ ; thus,  $A = A_0 \cup (e + A_1) \cup \dots \cup (4e + A_4)$ . Having  $A$  replaced with its appropriate translate, we can assume that  $A_0$  has density larger than 0.5 in  $F$ , whence  $2A_0 = F$  by Lemma 1. If now  $A_i$  is non-empty for some  $i \in [1, 4]$ , then  $ie + F = (ie + A_i) + 2A_0 \subseteq 3A$ . This shows that at least one of the sets  $A_i$  is empty. Moreover, we can assume that *exactly* one of them is empty, as otherwise the proof is over. Replacing  $e$  with one of  $2e, 3e$ , or  $4e$ , is necessary, we assume that  $A_4 = \emptyset$  while  $A_i \neq \emptyset$  for  $i \in [1, 3]$ , and aim to obtain a contradiction. Notice, that

$$A = A_0 \cup (e + A_1) \cup (2e + A_2) \cup (3e + A_3),$$

and that  $ie + F \subseteq 3A$  for each  $i \in [1, 3]$  by the observation above, implying  $4e + F \not\subseteq 3A$ . The last condition yields

$$A_0 + ((A_1 + A_3) \cup 2A_2) \neq F, \quad (2)$$

and it follows from Lemma 1 that

$$|A_0| + |(A_1 + A_3) \cup 2A_2| \leq |F|. \quad (3)$$

Notice, that the last estimate implies  $|2A_2| \leq |F| - |A_0| < 0.5|F|$ , whence

$$|A_2| < 0.25|F| \quad (4)$$

by Lemma 3.

Let  $H$  be the period of the left-hand side of (2); thus,  $H$  is a proper subgroup of  $F$ , and we claim that, in fact,

$$|H| \leq 5^{-2}|F|. \quad (5)$$

To see this, suppose for a contradiction that  $|F/H| = 5$ . Denote by  $\varphi_H$  the canonical homomorphism  $\mathbb{Z}_5^n \rightarrow \mathbb{Z}_5^n/H$ . From  $|A_0| > 0.5|F|$  we conclude that  $|\varphi_H(A_0)| \geq 3$ , and then (2) along with Lemma 1 shows that

$$|\varphi_H((A_1 + A_3) \cup 2A_2)| \leq 5 - |\varphi_H(A_0)| \leq 2.$$



This gives  $|\varphi_H(A_2)| = 1$ ,  $\min\{|\varphi_H(A_1)|, |\varphi_H(A_3)|\} = 1$ , and  $\max\{|\varphi_H(A_1)|, |\varphi_H(A_3)|\} \leq 5 - |\varphi_H(A_0)|$ . As a result,

$$|\varphi_H(A_0)| + |\varphi_H(A_1)| + |\varphi_H(A_2)| + |\varphi_H(A_3)| \leq 7,$$

implying  $|A| = |A_0| + |A_1| + |A_2| + |A_3| \leq 7|H| < 1.5|F|$ , contrary to the density assumption. This proves (5).

Since  $\pi((A_1 + A_3) \cup 2A_2) \leq H$  by the definition of the subgroup  $H$ , applying subsequently Lemma 2 and then Kneser's theorem we obtain

$$\begin{aligned} |(A_1 + A_3) \cup 2A_2| &\geq \min\{|A_1 + A_3| + |\pi(A_1 + A_3)|, |2A_2| + |\pi(2A_2)|\} - |H| \\ &\geq \min\{|A_1| + |A_3|, 2|A_2|\} - |H|. \end{aligned} \quad (6)$$

If  $|A_1| + |A_3| \leq 2|A_2|$ , then from (3), (6), (4), and (5),

$$\begin{aligned} |F| &\geq |A_0| + |A_1| + |A_3| - |H| = |A| - |A_2| - |H| \\ &> \frac{3}{2}|F| - \frac{1}{4}|F| - \frac{1}{25}|F| = \frac{121}{100}|F|, \end{aligned}$$

a contradiction. Thus, we have

$$|A_1| + |A_3| > 2|A_2|$$

and then

$$|A_0| + 2|A_2| \leq |F| + |H|$$

by (3) and (6). The latter estimate gives

$$\frac{3}{2}|F| < |A| = |A_0| + |A_1| + |A_2| + |A_3| \leq \frac{|F| + |H|}{2} + \frac{|A_0|}{2} + |A_1| + |A_3|,$$

whence

$$\frac{1}{2}|A_0| + |A_1| + |A_3| > |F| - \frac{1}{2}|H|.$$

Using again (3) and applying Kneser's theorem, we now obtain

$$\begin{aligned} |F| &\geq |A_0| + |A_1 + A_3| \geq |A_0| + |A_1| + |A_3| - |\pi(A_1 + A_3)| \\ &> \frac{1}{2}|A_0| + |F| - \frac{1}{2}|H| - |\pi(A_1 + A_3)| \end{aligned}$$

leading, in view of (5), to  $|\pi(A_1 + A_3)| \geq (|A_0| - |H|)/2 > |F|/5$  and thus to  $\pi(A_1 + A_3) = F$ . This, however, means that  $A_1 + A_3 = F$ , contradicting (2).  $\square$

Propositions 1 and 2 show that to establish Theorem 5, it suffices to consider sets  $A \subseteq \mathbb{Z}_5^n$  with density smaller than 0.5 in every coset of every index-5 subgroup.

**Lemma 4.** *Let  $n \geq 1$  be an integer, and suppose that  $A, B, C \subseteq \mathbb{Z}_5^n$  are subsets of densities  $\alpha, \beta$ , and  $\gamma$ , respectively. If  $0.4 < \alpha, \beta < 0.5$  and  $\alpha + \beta + 3\gamma > 1.5$ , then  $A + B + C = \mathbb{Z}_5^n$ .*

*Proof.* Let  $H := \pi(A + B + C)$ ; assuming that  $H \neq \mathbb{Z}_5^n$ , we obtain a contradiction. As above, let  $\varphi_H: \mathbb{Z}_5^n \rightarrow \mathbb{Z}_5^n/H$  denote the canonical homomorphism.

If  $|\mathbb{Z}_5^n/H| = 5$  then, in view of  $|A|/|H| = 5\alpha > 2$  we have  $|\varphi_H(A)| \geq 3$ . Similarly,  $|\varphi_H(B)| \geq 3$ , and it follows that  $\varphi_H(A) + \varphi_H(B) = \mathbb{Z}_5^n/H$ ; that is,  $A + B + H = \mathbb{Z}_5^n$ . Hence,  $A + B + C = (A + B + H) + C = \mathbb{Z}_5^n$ , contradicting the assumption  $H \neq \mathbb{Z}_5^n$ .

If  $|\mathbb{Z}_5^n/H| \geq 125$  then, by Kneser's Theorem and taking into account that

$$\pi(A + B) \leq \pi(A + B + C) = H, \quad (7)$$

we have

$$\begin{aligned} |A + B + C| &\geq |A + B| + |C| - |H| \\ &\geq |A| + |B| + |C| - 2|H| \\ &= \frac{2}{3}|A| + \frac{2}{3}|B| + \frac{1}{3}(|A| + |B| + 3|C|) - 2|H| \\ &> \left( \frac{2}{3} \cdot 0.4 + \frac{2}{3} \cdot 0.4 + \frac{1}{3} \cdot 1.5 - \frac{2}{125} \right) \cdot 5^n \\ &> 5^n, \end{aligned}$$

a contradiction.

Finally, consider the situation where  $|\mathbb{Z}_5^n/H| = 25$ . In this case  $|A|/|H| = 25\alpha > 10$  whence  $|A + H| \geq 11|H|$  and similarly,  $|B + H| \geq 11|H|$ . In view of (7), Kneser's Theorem gives

$$|A + B + H| = |(A + H) + (B + H)| \geq |A + H| + |B + H| - |H| \geq 21|H|.$$

Also,

$$|C|/|H| = 25\gamma > \frac{25}{3}(1.5 - \alpha - \beta) > \frac{25}{6} > 4.$$

Consequently,  $|C + H| \geq 5|H|$  and therefore

$$|A + B + H| + |C + H| \geq 26|H| > 5^n.$$

Lemma 1 now implies  $A + B + C = (A + B + H) + (C + H) = \mathbb{Z}_5^n$ , contrary to the assumption  $H \neq \mathbb{Z}_5^n$ .  $\square$

**Proposition 3.** *Let  $n \geq 1$  be an integer, and suppose that  $A \subseteq \mathbb{Z}_5^n$  is a subset of density larger than 0.3, such that  $3A \neq \mathbb{Z}_5^n$ . If  $F < \mathbb{Z}_5^n$  is an index-5 subgroup with the density of  $A$  in every  $F$ -coset smaller than 0.5, then there is at most one  $F$ -coset where the density of  $A$  is larger than 0.4.*

*Proof.* Suppose for a contradiction that there are two (or more)  $F$ -cosets containing more than  $0.4|F|$  elements of  $A$  each. Shifting  $A$  and choosing  $e \in \mathbb{Z}_5^n \setminus F$  appropriately, we can then write  $A = A_0 \cup (e + A_1) \cup (2e + A_2) \cup (3e + A_3) \cup (4e + A_4)$  with  $A_0, A_1, A_2, A_3, A_4 \subseteq F$  satisfying  $\min\{|A_0|, |A_1|\} > 0.4|F|$ .

By Lemma 4 (applied to the group  $F$ ), we have

$$3A_0 = 2A_0 + A_1 = A_0 + 2A_1 = 3A_1 = F,$$

implying  $F \cup (e + F) \cup (2e + F) \cup (3e + F) \subseteq 3A$  and, consequently,  $4e + F \not\subseteq 3A$  by the assumption  $3A \neq \mathbb{Z}_5^n$ . Furthermore, if we had  $2|A_0| + 3|A_4| > 1.5|F|$ , this would imply  $2A_0 + A_4 = F$  by Lemma 4, resulting in  $4e + F \subseteq 3A$ ; thus,

$$2|A_0| + 3|A_4| < 1.5|F|. \quad (8)$$

Similarly,

$$|A_0| + |A_1| + 3|A_3| < 1.5|F| \quad (9)$$

and

$$2|A_1| + 3|A_2| < 1.5|F| \quad (10)$$

(as otherwise by Lemma 4 we would have  $A_0 + A_1 + A_3 = F$  and  $2A_1 + A_2 = F$ , respectively, resulting in  $4e + F \subseteq 3A$ ). Adding up (8)–(10) we obtain

$$|A| = |A_0| + |A_1| + |A_2| + |A_3| + |A_4| < 1.5|F| = 0.3 \cdot 5^n,$$

contrary to the assumption on the density of  $A$ .  $\square$

We now use Fourier analysis to complete the argument and prove Theorem 5.

Suppose that  $n \geq 2$ , and that a set  $A \subseteq \mathbb{Z}_5^n$  has density  $\alpha > 0.3$  and satisfies  $3A \neq \mathbb{Z}_5^n$ ; we want to show that  $A$  is contained in a union of two cosets of an index-5 subgroup. Having translated  $A$  appropriately, we can assume that  $0 \notin 3A$ . Denoting by  $1_A$  the indicator function of  $A$ , consider the Fourier coefficients

$$\hat{1}_A(\chi) := 5^{-n} \sum_{a \in A} \chi(a), \quad \chi \in \widehat{\mathbb{Z}_5^n}.$$

For every character  $\chi \in \widehat{\mathbb{Z}_5^n}$ , find a cube root of unity  $\zeta(\chi)$  such that, letting  $z(\chi) := -\hat{1}_A(\chi)\zeta(\chi)$ , we have  $\Re(z(\chi)) \geq 0$ . The assumption  $0 \notin 3A$  gives

$$\sum_{\chi} (\hat{1}_A(\chi))^3 = 0.$$

Consequently,

$$\sum_{\chi \neq 1} \Re((z(\chi))^3) = \Re\left(\sum_{\chi \neq 1} (-\hat{1}_A(\chi))^3\right) = \alpha^3,$$

and since  $\Re(z) \geq 0$  implies  $\Re(z^3) \leq |z|^2 \Re(z)$  (as one can easily verify), it follows that

$$\sum_{\chi \neq 1} |z(\chi)|^2 \Re(z(\chi)) \geq \alpha^3.$$

Comparing this to

$$\sum_{\chi \neq 1} |z(\chi)|^2 = \alpha(1 - \alpha)$$

(which is an immediate corollary of the Parseval identity), we conclude that there exists a non-principal character  $\chi$  such that

$$\Re(z(\chi)) \geq \frac{\alpha^2}{1 - \alpha}. \quad (11)$$

In view of  $\alpha > 0.3$ , it follows that  $\Re(-\hat{1}_A(\chi)\zeta(\chi)) > \frac{9}{70}$ .

Replacing  $\chi$  with the conjugate character, if needed, we can assume that  $\zeta(\chi) = 1$  or  $\zeta(\chi) = \exp(2\pi i/3)$ . Let  $F := \ker \chi$ , fix  $e \in \mathbb{Z}_5^n$  with  $\chi(e) = \exp(2\pi i/5)$ , and for each  $i \in [0, 4]$ , let  $\alpha_i$  denote the density of  $A - ie$  in  $F$ . By Propositions 1 and 2, we can assume that  $\max\{\alpha_i : i \in [0, 4]\} < 0.5$ , and then by Proposition 3 we can assume that there is at most one index  $i \in [0, 4]$  with  $\alpha_i > 0.4$ ; that is, of the five conditions  $\alpha_i \leq 0.4$  ( $i \in [0, 4]$ ), at most one may fail to hold and must be relaxed to  $\alpha_i < 0.5$ . We show that these assumptions are inconsistent with (11). To this end, we consider two cases.

Case (i):  $\zeta(\chi) = 1$ . In this case we have

$$\alpha_0 + \alpha_1 \cos(2\pi/5) + \cdots + \alpha_4 \cos(8\pi/5) = 5\Re(\hat{1}_A(\chi)) < -\frac{9}{14}. \quad (12)$$

For each  $k \in [0, 4]$ , considering  $\alpha_0, \dots, \alpha_4$  as variables, we now minimize the left-hand side of (12) under the constraints

$$\alpha_0 + \cdots + \alpha_4 \geq 1.5, \quad (13)$$

$$\alpha_k \in [0, 0.5], \quad (14)$$

and

$$\alpha_i \in [0, 0.4] \text{ for all } i \in [0, 4], \ i \neq k. \quad (15)$$

This is a standard linear optimization problem which can be solved precisely, and computations show that for every  $k \in [0, 4]$ , the smallest possible value of the expression under consideration exceeds  $-9/14$ . This rules out Case (i).

Case (ii):  $\zeta(\chi) = \exp(2\pi i/3)$ . In this case we have

$$\sum_{j=0}^4 \alpha_j \cos \left( 2\pi \left( \frac{1}{3} + \frac{j}{5} \right) \right) = 5\Re(\hat{1}_A(\chi) \exp(2\pi i/3)) < -\frac{9}{14}. \quad (16)$$

Minimizing the left-hand side of (16) under the constraints (13)–(15), we see that its minimum is larger than  $-9/14$ . This rules out Case (ii), completing the proof of Theorem 5.

#### 4. FROM $\mathbf{t}_\rho^+(G)$ TO $\mathbf{N}_k(G)$

In Section 1, we mentioned the close relation between the quantity  $\mathbf{N}_k(G)$  and an invariant introduced in [KL09]. Denoted by  $\mathbf{t}_\rho^+(G)$  in [KL09], this invariant was defined for integer  $\rho \geq 1$  and a finite abelian group  $G$  to be the largest size of an aperiodic generating subset  $A \subseteq G$  such that  $(\rho - 1)(A \cup \{0\}) \neq G$  and  $A$  is maximal under this condition. It was shown in [KL09] that  $\mathbf{t}_\rho^+(G) = 0$  if  $\rho > \text{diam}^+(G)$ , while otherwise  $\mathbf{t}_\rho^+(G)$  is the largest size of an aperiodic subset  $A \subseteq G$  satisfying  $(\rho - 1)(A \cup \{0\}) \neq G$  and maximal under this condition. Our goal in this section is to prove the following simple lemma allowing one to “translate” the results of [KL09] into our present Theorems 2–4.

**Lemma 5.** *For any finite abelian group  $G$  and integer  $k \geq 1$ , we have*

$$\mathbf{t}_{k+1}^+(G) = \mathbf{N}_k(G), \quad (17)$$

*except if  $|G|$  is prime and  $k \geq |G| - 1$ , in which case  $\mathbf{t}_{k+1}^+(G) = 0$  and  $\mathbf{N}_k(G) = 1$ .*

*Proof.* We show that (17) holds true unless  $k \geq \text{diam}^+(G)$  and  $|G|$  is prime; the rest follows easily.

Let  $\mathcal{G}$  denote the set of all aperiodic subsets  $A \subseteq G$ , and let  $\mathcal{G}_0$  be the set of all aperiodic subsets  $A \subseteq G$  with  $0 \in A$ .

Since translating a set  $A \subseteq G$  affects neither its periodicity, nor the property  $kA = G$ , we have

$$\mathbf{N}_k(G) = \max\{|A| : A \in \mathcal{G}_0, kA \neq G, k(A \cup \{g\}) = G \text{ for each } g \in G \setminus A\}.$$

As a trivial restatement,

$$\begin{aligned} \mathbf{N}_k(G) = \max\{|A| : A \in \mathcal{G}_0, k(A \cup \{0\}) \neq G, \\ k(A \cup \{0\} \cup \{g\}) = G \text{ for each } g \in G \setminus A\}. \end{aligned} \quad (18)$$

However, letting  $g = 0$  shows that the conditions

$$k(A \cup \{0\}) \neq G \text{ and } k(A \cup \{0\} \cup \{g\}) = G \text{ for each } g \in G \setminus A$$

automatically imply  $0 \in A$ . Thus, in (18), the assumption  $A \in \mathcal{G}_0$  can be replaced with  $A \in \mathcal{G}$ , meaning that  $\mathbf{N}_k(G)$  is the largest size of an aperiodic subset  $A \subseteq G$  satisfying  $k(A \cup \{0\}) \neq G$  and maximal under this condition; consequently, taking into account the discussion at the beginning of this section, if  $k < \text{diam}^+(G)$ , then  $\mathbf{N}_k(G) = \mathbf{t}_{k+1}^+(G)$ .

Consider now the situation where  $k \geq \text{diam}^+(G)$ . In this case  $\mathbf{t}_{k+1}^+(G) = 0$ , and by the definition of  $\text{diam}^+(G)$ , for any generating subset  $A \subseteq G$  we have  $k(A \cup \{0\}) = G$ . Suppose that  $A \in \mathcal{G}$  satisfies  $kA \neq G$  and is maximal subject to this condition. (If such sets do not exist, then  $\mathbf{N}_k(G) = 0 = \mathbf{t}_{k+1}^+(G)$ .) Translating  $A$  appropriately, we can assume that  $0 \in A$ , and then  $k(A \cup \{0\}) = kA \neq G$ . It follows that  $A$  is not generating; that is,  $H := \langle A \rangle$  is a proper subgroup of  $G$ . Furthermore, the maximality of  $A$  shows that  $A = H$  is a maximal subgroup, and aperiodicity of  $A$  gives  $A = H = \{0\}$ . Therefore  $G$  has prime order.  $\square$

## REFERENCES

- [B15] B. BAJNOK, The  $h$ -critical number of finite abelian groups, *Uniform Distribution Theory* **10** (2015), no. 2, 93–115.
- [DT89] A.A. DAVYDOV and L.M. TOMBAK, Quasiperfect linear binary codes with distance 4 and complete caps in projective geometry (Russian), *Problemy Peredachi Informatsii* **25** (1989), no. 4, 11–23; translation in *Problems Inform. Transmission* **25** (1989), no. 4, 265–275 (1990).
- [KL09] B. KLOPSCH and V.F. LEV, Generating abelian groups by addition only, *Forum Mathematicum* **21** (2009), no. 1, 23–41.
- [Kn53] M. KNESER, Abschätzung der asymptotischen Dichte von Summenmengen, *Math. Z.* **58** (1953), 459–484.
- [Kn55] ———, Ein Satz über abelsche Gruppen mit Anwendungen auf die Geometrie der Zahlen, *Math. Z.* **61** (1955), 429–434.

*E-mail address:* `seva@math.haifa.ac.il`

DEPARTMENT OF MATHEMATICS, THE UNIVERSITY OF HAIFA AT ORANIM, TIVON 36006, ISRAEL